EXHIBIT H

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,	°	
Plaintiff and Counterclaim-Defendant	°	
v.	°	C.A. No. 04-1199 (SLR)
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation,	°	
Defendants and Counterclaim-Plaintiffs	°	

VIDEOTAPED ORAL DEPOSITION OF

DANIEL M. TEAL

May 24, 2006

REPORTED BY: SUSAN P. MILLER, RDR, CRR, CBC

I do know that they received some funding from the U.S. Government for their research.

Q. Does the U.S. Government fund work on research that's directed to problems that have already been solved? 08:32:48

A. I cannot comment on if the U.S. Government is funding problems that have already been solved.

Q. Does that seem reasonable to you?

MS. BROWN: Objection, calls for speculation. 08:32:58

A. Again, it all depends upon how you define if the problem is solved or not. Again, I do not know if the government is funding problems that have already been solved. It also depends: Has the problem been solved? I'm not aware. If you could point out a specific problem that I could answer -- I mean, that's a very vague question. 08:33:14

Q. (BY MR. MILLER) You say that NetRanger solved the problems that EMERALD purportedly solved, but did it several years earlier. Isn't that your opinion? 08:33:29

MS. BROWN: Objection, vague.

A. I produced -- we sold NetRanger several years prior to publication of the EMERALD paper as 08:33:48

it was a successful product. The U.S. government, it was whether they funded EMERALD, if they thought NetRanger may have solved it, that was up to them.

Q. (BY MR. MILLER) So you think the government funded EMERALD work to the tune of millions of dollars when they could have gone out and bought a commercial NetRanger product. That makes sense to you? 08:34:08

MS. BROWN: Objection, vague, calls for speculation. Also, lacks foundation, vague as to what you mean by "the EMERALD project." 08:34:21

Q. (BY MR. MILLER) Do you understand the question?

A. I would like to point out that the U.S. Government did purchase NetRanger systems. You know, if they continued funding the EMERALD project, that may have been another part of the U.S. Government. 08:34:31

Q. Okay. Let's try to answer my question. Does it make sense to you that the government would have funded EMERALD research if your commercial NetRanger product already solved the problems that the EMERALD research was directed to? 08:34:45

MS. BROWN: Objection, vague as to "EMERALD research." 08:34:59

A. Let me point out, NetRanger was a successful commercial product. The U.S. Government purchased it. They may have funded EMERALD for continued research for doing things in a different way, maybe, that... 08:35:17

Going ahead and dealing with, for example, statistical detection, which in 1997 was not viable for commercial systems.

Q. (BY MR. MILLER) Statistical anomaly detection was not viable for commercial systems; 08:35:43 that's your opinion?

A. In my opinion, in 1997, I was not aware of any statistical anomaly detection system that would have worked in a commercial setting.

Q. Before becoming involved in this lawsuit, 08:36:06 had you ever heard anyone say that SRI's work in the intrusion detection field was not of high quality?

A. That depends upon the definition of "high quality." Are you talking about high quality for a research project, or high quality for a 08:36:27 commercial-grade product that could be sold on the open market?

Q. Let's start with commercial -- I'm sorry. Let's start with research project.

A. I am aware that SRI produced, you know, 08:36:41

for the IDES project and the NIDES project research systems that were used in limited research settings. They probably tested it at one site. Other than that, I cannot comment on -- you know, they may not have tested it at all. I do not know if they tested it at one or more sites. 08:37:05

I never used the IDES system. I never used the NIDES system. I never used the EMERALD system. They presented lots of papers at computer security conferences on the research that they performed. 08:37:23

Q. Did you ever hear anybody criticize or speak negatively of SRI's work in the intrusion detection field?

MS. BROWN: Objection, calls for speculation. 08:37:33

A. I have never heard individuals in the computer security field comment negatively on the IDES or any other research project, to my recollection. They were research projects. It depends upon comment negatively -- I never heard anyone say that, "Oh, this cannot be used for a commercial system," although that was my opinion. But I never heard anyone say that at a conference. 08:37:56

Q. (BY MR. MILLER) Did you ever hear anyone 08:38:14

say anything negative about SRI's research in the intrusion detection field?

A. I can't remember anyone saying anything negative about SRI's research.

Q. Do you recall ever hearing anyone say that SRI was taking credit for work that was not done by SRI? 08:38:30

A. I could not comment on that. I don't remember anyone saying, you know, that SRI's taking credit for other people's work at those research conferences. 08:38:50

Q. Why did you keep the IDES, NIDES and EMERALD articles in your files?

A. I keep lots of files just because I am -- I do work in the computer security field, and I keep files just to have them. 08:39:18

Q. You keep files on useless work?

A. I keep files -- well, that depends upon if I believe -- in terms of useless work, I may have stuff, but it depends upon -- in which case it was presented at a research conference, I kept copies of it. I have proceedings from lots of technical conferences. So I just have a habit of keeping all the papers, or as many papers as I can keep, from technical conferences or, you know, research 08:39:35 08:39:57

projects that were presented at the conferences.

Q. In your invoice, you note that you spent five hours preparing documents to produce in response to SRI's subpoena to you.

A. Yes, I spent approximately five hours searching through everything. 08:40:17

Q. So what did you do in the five hours?

A. In the five hours, I spent at least an hour going through all of the conference proceedings that I've had. May have been more time than that. 08:40:35 I also spent time researching -- you know, getting all of the files for WheelGroup Corporation and NetRanger that were also requested by the subpoena. That took probably more time than going through all of my files looking for papers regarding SRI. 08:40:59

Q. Were there any papers relating to WheelGroup or NetRanger that you didn't produce?

A. I produced all of the files that were requested, everything except source code to NetRanger. 08:41:20

Q. You have the source code for NetRanger?

A. I have some source code for NetRanger.

Q. Which source -- for which version of NetRanger do you have source code?

A. I have source code for Version 1.0; some 08:41:36

internal research versions for the time frame between 1.0 and 2.0, not complete, but some of the source. I have source code for some of the versions -- you know, for, basically, 2.0; basically, test stuff. I did not maintain the complete set of source code, for example, for 1.3 or 2.0. 08:42:01

Q. I noticed in some of your documents actually attached to your report that WheelGroup did consulting for its customers. Is that correct? 08:42:23

A. Yes, WheelGroup did do consulting for some of our customers.

Q. Do you have any documents relating to that consulting work in your files?

A. I believe I produced a number of documents in regards to the subpoena for that consulting work. I don't remember exactly which ones. I was just finding files and copying them over. Those files were produced a long time ago. I did not read them in response to providing them for the subpoena. 08:42:36 08:42:56

Q. They were produced, meaning they were created a long time ago?

A. They were created when WheelGroup -- over 10 years ago. 08:43:10

Q. When you were reviewing the documents for production, do you recall any documents that reflected or depicted a customer's network architecture?

A. I don't specifically recall. There may have been. 08:43:31

Q. If there was such a document in your files --

A. If there was -- there may have been a document. There may not have. I do not know if there was a document that depicted a customer's architecture. 08:43:40

Q. If there was such a document, you would have produced it?

A. If there was a document with a customer's network architecture, I would have produced it. 08:43:49

Q. You mentioned previously that there may have been some testing of IDES and NIDES. Are you aware of any testing of the EMERALD system, any of the EMERALD systems? 08:44:11

A. I am not aware of any testing of the EMERALD systems. I read those papers a long time ago. They may have referred to it. They may not. I do not remember.

Q. You looked for a paper regarding Lincoln 08:44:32

question is yes?

MS. BROWN: Objection, asked and answered.

A. Yes, you could provide, an API allows you -- you could do that. 09:23:22

Q. (BY MR. MILLER) You could transform from one form --

A. Yeah. Yeah. Yeah. It depends upon a definition of what you're trying to do with the transforming more at the technical level, but... 09:23:31

Q. So just let me ask the question more cleanly and you can answer it: Can an API allow the system to transform data from one form into another form?

MS. BROWN: Objection, vague as to whether you're speaking generally or in the context of the patents. 09:23:43

A. The answer is yes. And based on that definition, my NetRanger system did that.

MR. MILLER: Let's take a break. 09:23:56

THE VIDEOGRAPHER: We're off the record at 9:23 a.m. This is the end of Tape No. 1.

(Recess taken at 9:23 a.m.)

THE VIDEOGRAPHER: Stand by, please. We're back on the record at 9:34 a.m. This is the 09:34:42

beginning of Tape No. 2.

Q. (BY MR. MILLER) Back in September, approximately September of last year when you first skimmed the patents-in-suit, what were your impressions? 09:34:55

A. My impressions? My initial impression is that the patent -- you know, based on the face of it, that I'd already done lot of that with NetRanger. A lot, maybe all of it. I don't remember. I mean, in which case I had my NetRanger system out there, and I saw this was filed long after we were selling NetRanger on the market. 09:35:14

Q. Is there anything described by the patents-in-suit that you don't believe you invented?

MS. BROWN: Objection, calls for a legal conclusion. Are you speaking of claims or the description? It's vague. Are you going to place the patent in front of the witness? 09:35:28

A. The -- I don't remember my thoughts at the time. What I do remember in the patent is the patents, one of them, did cover signature detection, misuse detection, okay, which is what NetRanger did; did it very well. 09:35:44

The patents also address statistical anomaly detection, which NetRanger did not do and 09:35:58

did not do for commercial reasons because in my opinion, and it's still my opinion today, that statistical analysis is more for research-type products rather than a commercial product.

Q. (BY MR. MILLER) Are you familiar with Symantec's products? 09:36:14

A. I am not familiar with Symantec's intrusion detection products. I did not look at them in regards to this case.

Q. Were you asked to take a look at Symantec's intrusion detection products? 09:36:24

A. I was not asked to take a look at Symantec's intrusion detection products.

Q. Do you know whether Symantec's intrusion detections include any statistical anomaly detection? 09:36:36

A. I do --

MS. BROWN: Objection, calls for speculation.

A. I do not know if they include it or not. 09:36:42

Q. (BY MR. MILLER) Do you know whether ISS' products include statistical anomaly detection?

A. I --

MS. BROWN: Objection, calls for speculation. 09:36:54

Mr. Teal, you have to just pause and let me get my objections on the record, please. Okay.

THE WITNESS: Okay.

A. No, I do not know if they include statistical detection or not. It also depends upon what you define as "statistical detection." For example, some misuse detection might be construed as statistical detection. 09:36:58

"Statistical detection" over the years has seemed to have had many different meanings, and it's a very broad term, and it appears to -- it can mean many different things. 09:37:11

Q. (BY MR. MILLER) In the context of the '212 patent, what do you believe it means? If you'd take a look at Exhibit E to your report. 09:37:22

A. For the '212 patent -- for which part of Exhibit E?

Q. Take a look at page 57 of Exhibit E to your report. Are you there? 09:37:57

A. Yes. I see page 57.

Q. Okay. And you understand that page 57 is addressing claim 1 of SRI's '212 patent?

A. At page 57, it says, "See '203, claim 1."

Q. Okay. Do you understand that page 57 is 09:38:29

addressing claim 1 of the '212 patent, or not?

A. I don't understand your question because I'm looking at page 57 and on there, in my expert report, I say, "See '203, claim 1."

Q. Did you prepare this claim chart, Exhibit E? 09:38:49

A. The draft of this claim chart was produced by my legal counsel, upon discussions with myself, and I reviewed it claim-by-claim with the legal counsel. 09:39:01

Q. Do you recognize any claim of the '212 patent on page 57?

MS. BROWN: Objection, vague as to "recognize." Are you going to place the '212 patent in front of him, Counsel? Are you asking him to make a comparison? 09:39:13

A. There, for the '212 claim number, going through, after reviewing the claim in '212, I reference and said we've already covered this in '203, claim 1. 09:39:38

Q. (BY MR. MILLER) Okay. Do you recognize claim 1 of the '212 patent on page 57?

MS. BROWN: Objection, vague as to "recognize."

A. On the '212, the only difference is where 09:39:50

A. Yes.
Q. And you say that a statistical detection method could be any of the three proposed constructions?
A. That is correct. 09:41:21
Q. In your -- in reaching your conclusions as to whether or not that limitation, "Wherein at least one of the network monitors uses a statistical detection method" -- in analyzing whether or not that limitation was present in the prior art, did 09:41:38 you use one of these three constructions, your own construction, or something else?
MS. BROWN: Objection, asked and answered.
A. I used all three constructions for my 09:41:51 answer.
Q. (BY MR. MILLER) Earlier today you mentioned that you're a named inventor on a number of patents?
A. Yes. 09:42:10
Q. Do you know how many?
A. Five patents, to my knowledge.
Q. These are all patents that are assigned to Cisco?
A. That is correct. Cisco does -- is the 09:42:21

assignee for those five patents.

Q. Were any of the five patents on which you're listed as a named inventor filed before the SRI patents-in-suit?

MS. BROWN: Objection, calls for speculation. 09:42:37

A. I do not know the dates of when they were filed and if it was before or after the SRI patents.

Q. (BY MR. MILLER) When were the SRI patents-in-suit filed? 09:42:46

MS. BROWN: Objection, calls for speculation. You haven't placed the patents in front of him.

A. I don't remember the exact dates that the SRI patents were filed. 09:42:55

(Exhibit 463 marked/introduced.)

Q. (BY MR. MILLER) Mr. Teal, the reporter has placed before you Exhibit 463, which is identified as TEA_17 through 34. It's U.S. Patent 630,668. Do you recognize this document? 09:43:28

A. Yes, that is one of my patents.

Q. And your name is there on the front, Daniel M. Teal?

A. That is me, yes.

Q. Why didn't you tell the Patent Office 09:43:40

about any of SRI's work in intrusion detection?

A. For the --

MS. BROWN: Objection, lacks foundation.

Q. (BY MR. MILLER) Okay. Did you tell the Patent Office about any of SRI's work in intrusion detection during the prosecution of this patent? 09:43:53

A. I do not -- I do not know, because I did not contact the Patent Office. I was working with Cisco Systems' law firm. I do not remember their name. This was a number of years ago. They may have provided it, they may have not. I gave a number of papers in support of the work for this patent. I do not remember the list of all the papers that I presented. 09:44:06 09:44:25

Q. Take a look at the first couple of pages of the patent.

A. Okay.

Q. So page 18, page 19, page 20, page 21 -- I'm referring to the TEA numbers on there. 09:44:44

A. Oh, the TEA numbers. Okay.

Q. Yeah. So it's like the first --

A. Okay.

Q. -- four pages of the patent.

A. Uh-huh. 09:44:51

Q. Actually, first five pages of the patent. You see a whole bunch of prior art references identified there?

A. Yes, I do.

Q. Do you see any SRI documents identified there? 09:45:01

A. I would have to read through all the listings. There's a number of them here. If there's some you'd like to point out to me --

Q. I can't. I'll represent to you I don't see any SRI publications. 09:45:12

(Witness reviewing document(s).)

A. So none there. And, more than likely, I probably did not, you know, provide any of the SRI papers because they deal with statistical detection, which is not a commercially viable solution; and at Cisco, we did not depend upon statistical detection. So, therefore, in my opinion, the SRI documents were irrelevant for my patents. 09:45:34

Q. (BY MR. MILLER) The SRI research was not material to the NetRanger work or the Cisco products? 09:45:55

A. They told me what not to do.

Q. Okay. Is it your testimony that the SRI documents don't discuss statistical analysis at all? 09:46:04

I'm sorry. Withdrawn.

Is it your testimony that the SRI documents don't discuss signature analysis at all?

MS. BROWN: Objection, lacks foundation, vague as to which document you're referring to. 09:46:16

A. At the -- I do not remember at the time that I was providing information in support of this patent. And just for the record, I left Cisco soon after providing initial stuff, so I don't know, you know, that whole process after I left. 09:46:35

I was not aware -- I do not remember if there was SRI documents. I do not remember SRI having signature analysis in their work.

Q. (BY MR. MILLER) Are you aware, as you sit here today, whether, for example, the EMERALD '97 paper that you cite to in your report discusses signature analysis? 09:46:56

A. I do not remember the whole contents of that paper. It may have. It may have not. 09:47:09

Q. You had the EMERALD '97 paper back in -- before -- at least before December of 1998, right?

MS. BROWN: Objection, calls for speculation.

A. I may have had a copy of it. 09:47:27

Q. (BY MR. MILLER) Why didn't you tell the Patent Office about NetRanger when you filed this application for this '668 patent?

MS. BROWN: Objection, lacks foundation. 09:47:42

A. Again, I did not talk to the Patent Office, so I do not know if the law firm told the Patent Office about NetRanger or not. I can't provide an answer on that.

Q. (BY MR. MILLER) Do you know whether the Patent Office told the -- withdrawn. 09:47:57

Do you know whether the law firm told the Patent Office about the SPOCK paper that you reference in your report?

A. I do not know if the law firm told the Patent Office about our SPOCK paper. 09:48:07

Q. What about the AFIWC assessment of NetRanger that you reference in your report? Did the law firm tell the Patent Office about that?

MS. BROWN: Objection, calls for speculation. 09:48:20

A. I do not know if the law firm provided that paper to the Patent Office.

Q. (BY MR. MILLER) You think NetRanger, SPOCK or AFIWC would be relevant to the 09:48:31

wasn't confidential. Is that correct?

MS. BROWN: Objection, calls for speculation.

A. I do not remember if I said it was confidential at that time or not, you know, in which case I remembered a DoD SPOCK report. I do not remember exactly when I provided, for example, the press release concerning the DoD SPOCK report. I had to go through and find a copy of that. I don't remember the exact date that I obtained it from Jerry Lathem. 10:19:55 10:20:15

Q. (BY MR. MILLER) All I'm trying to find out from you, sir, is about when you told the Symantec lawyers that you didn't believe the DoD SPOCK report was -- 10:20:31

A. It was probably in the September time frame.

Q. I didn't get my whole question out, so I need reask it, for the record.

A. Okay. 10:20:37

Q. So about when did you tell the Symantec lawyers that you did not believe the DoD SPOCK report was confidential?

MS. BROWN: Objection, calls for speculation, asked and answered. 10:20:48

A. I do not remember exactly when I told Symantec's lawyers that I thought that it was confidential [sic]. It may have been in September when I was discussing with it, and I have it on my hours right here. I don't remember the exact time. 10:21:01

Q. (BY MR. MILLER) Did you mean to say "not confidential"?

A. That makes it, yeah, not confidential, yes.

Q. Under "September 21," who's the former NetSolve employee that you called? 10:21:13

A. The former NetSolve employee was an individual by the name of Bob Gallen.

Q. G-O-W-E-N?

A. G-A -- no, Gallen, G-A-L -- how does he spell his last name? G-A-L-L-E-N, I believe. 10:21:38

Q. Thank you.

Did you do any work on this case and not bill for your time?

A. I would agree, yes, to that answer. 10:21:55

Q. How many hours did you work on the case and not bill?

A. I do not know the exact number of hours I did not bill. Again, I wasn't really doing this for the money. I just wrote it down, what I remembered, 10:22:11

because I figured they'd probably like an invoice from me at some point.

Q. Can't give me a ballpark?

A. Could have been 10 hours. Could have been 20 hours. I do not know. 10:22:22

Q. Did you do any activities that aren't noted on your time sheet?

MS. BROWN: Objection, vague as to "activities." Calls for speculation.

A. Yeah. I mean, I don't remember doing everything through here. The only individuals that I remember talking to were the ones that I had listed in my expert report or people -- you know, Bob Gallen at NetSolve, Todd Heberlein in April, I know, in going through and preparing the expert report, answering questions and so on. 10:22:39 10:23:09

Q. (BY MR. MILLER) Under "September 20," you have, "Canned database queries used in NetRanger." What does that mean?

A. Those were SQL scripts that were provided to customers with NetRanger that they could use stand-alone or the customers could modify to query a SQL database for generating and -- you know, lists of events, trying to correlate, as the example that I gave previously of looking that I have an attack 10:23:39 10:24:00

coming from a single source address, if I could write the SQL query such that if I want to find the number one source address that's attacking my network among all my multiple sensors.

That way, we know SQL queries would cover sequel queries based on space, which would be IP addresses; time, when events occurred; and type. You know, the types of alarms, i.e., all ping sweeps, port sweeps, that sort of thing. 10:24:15

Q. Okay. So the query is a question to the system? 10:24:28

A. Yes.

Q. Is that a fair characterization?

A. A query is you are -- not so much a question. It is going through the information that is in the system to produce a subset of data, and that's sorted in a useful manner. 10:24:38

Q. And then it generates a report?

A. It depends upon what you define by "report." The output to SQL queries would be outputted in -- could be in ASCII format. You could then put it into a file that you could put onto a piece of paper that could be construed as a report. 10:24:56

You could take the output from the SQL queries and feed that into shell scripts, if you 10:25:11

wanted to do further customization. You could take the output from the SQL queries and use that as feedback doing -- you know, additional -- as feedback, if you wanted to do additional queries.

Q. Using the NetRanger system, what could a user do with a SQL report? 10:25:23

MS. BROWN: Objection, calls for speculation, vague.

A. They could do just about anything that they wanted to. The key thing, one of the things that the customers liked about the NetRanger system is that we would produce all of the events that were generated by the NSX sensors and you could put them into an Oracle database, whether you had it go directly -- the system was so configurable, I could put them into an Oracle database directly from the NSX sensor, I could do it directly from a first-tier Director, I could do it directly from a second-tier Director. It all depends upon how the customer wanted to configure the system. 10:25:37 10:25:56 10:26:11

Once you generated all of these events, customers could then use them for historical purposes. They could use them to query for just about anything that they wanted. I mean, that's the power of the system. We generated events. You 10:26:23

know, we had timestamps of when an event occurred, type of event --

Q. (BY MR. MILLER) We've gone down that list.

A. Okay. 10:26:29

Q. A human operator would look at the output.

MS. BROWN: Objection, vague as to "output," calls for speculation.

A. You could have a human operator look at 10:26:39 the output. It was not required. It depends upon how you ran the SQL queries.

Q. (BY MR. MILLER) Are you aware of any deployment of NetRanger where a machine further processed the output of a query to perform automatic 10:26:53 correlation?

A. To the best of my recollection, I believe that the IBM emergency response services and NetSolve in their business models had automated SQL queries running on the system to generate stuff. 10:27:19

Q. They had the queries automated. I'm talking about processing, further processing of the query to do correlation. Are you aware of any deployment where the queries were further processed automatically by a computer to perform correlation? 10:27:38

MS. BROWN: Objection, vague, incomplete hypothetical, calls for speculation.

A. From that, I am aware that IBM and NetSolve had separate scripts that could run. It is the best of my recollection that they could take the output from that and run it through scripts, which could then be automated as to -- I do not have copies of those scripts. I do not have copies of the SQL queries that they ran. 10:27:55

I am aware that they liked using the NetRanger system because it's so configureable, they could do things like that. 10:28:13

Q. (BY MR. MILLER) Did Mr. Gallen provide you with any -- any information to support your view? 10:28:27

A. Mr. Gallen --

MS. BROWN: I'll just caution the witness, you need to wait until he finishes the question.

THE WITNESS: Okay. I'm sorry. 10:28:33

MS. BROWN: Just slow down there. Can you reask the question, please?

MR. MILLER: Sure.

Q. (BY MR. MILLER) Did Mr. Gallen tell you that NetSolve utilized a system that would 10:28:41

automatically take data provided in response to a query and perform machine-driven correlation on that data?

A. I do not remember Mr. Gallen telling me that when I talked to him in September. Mr. Gallen was not on -- a technical employee. He was in their -- -- I believe their sales or their biz-dev department at NetSolve. This is based upon my recollection from over 10 years ago when NetSolve was using the NetRanger product, so... 10:29:05 10:29:26

Q. Based on your recollection from over 10 years ago when NetSolve was using the NetRanger product, do you know of any specific example where NetSolve took the output of a SQL query and had a computer automatically process the data to perform correlation? 10:29:46

MS. BROWN: Objection, asked and answered.

A. I cannot remember a specific example. I remember people liked our system because they could do that with it. 10:29:59

Q. (BY MR. MILLER) Can you remember a specific example of the same data-processing done by IBM?

A. I cannot remember a specific example of 10:30:14

Q. Which part of NetRanger corresponds to the claimed hierarchical monitor?

A. That would be the NetRanger Director.

Q. Can NSX sensor correspond to the hierarchical monitor that's claimed? 12:42:04

A. The NSX sensor does not relate to the hierarchical monitors.

Q. Does NSX sensor report directly to HP OpenView?

MS. BROWN: Objection, vague as to "directly." 12:42:32

A. NSX sensor is configured to send event records, alarm records -- I use the terms interchangeably -- to the NetRanger Director to a piece of software that would take those messages and on that Director platform, insert them into HP OpenView. 12:42:51

Q. (BY MR. MILLER) So the answer to my question is: No, NSX sensor does not report directly to HP OpenView, correct? 12:43:18

MS. BROWN: Objection, misstates testimony. Also, vague.

A. The NSX sensor is sending alarms to the Director, which is then received by the system management interface daemon, which puts them into 12:43:33

HP OpenView.

Q. (BY MR. MILLER) Okay. Can NSX sensor send alarms to HP OpenView without going through Director?

A. The NSX sensor sends alarms through the SMI daemon, okay? It does not send it directly into HP OpenView. It sends them through that daemon into HP OpenView. 12:43:48

Q. Is the daemon in Director?

A. The system management interface is on the NetRanger Director. 12:44:08

Q. So the answer to my question, can NSX sensor send alarms to HP OpenView without going through Director is no, right?

A. I'm trying to understand your question where you state, can it send it without going through the Director. 12:44:27

Q. Right. If the daemon is part of Director and it has -- the event record has to go through the daemon to get to HP OverView, then the answer to my question is no, correct? 12:44:40

A. It has to go through the daemon, but it depends upon what you are defining as a director. If you are talking about the entire computer system with the operating system, the daemon, HP OpenView, 12:44:54

the answer is yes, it sends it directly there. If you are talking about the HP OpenView software application by itself, then the answer is it does not send it directly to that; it sends it to the Director platform. It all depends upon your definition of what the Director is. 12:45:09

Q. What, in your view, does "automatically" mean in the context of the claim limitation "automatically receiving and integrating reports of suspicious activity by one or more hierarchical monitors"? 12:45:31

A. "Automatically" would mean without user intervention.

Q. How is "integrating" different from "correlating," as claimed? 12:45:49

A. That is a very good question. And, to be honest, in times I have used the two terms, "integrate" and "correlate," similarly in speaking about NetRanger.

Q. For purposes of your analysis of the validity of the claims of the patents-in-suit, did you use the terms "integrating" and "correlating" interchangeably? 12:46:09

MS. BROWN: Objection, vague.

A. I do not remember if I did. I will state 12:46:25

that on this part here, you know, I have in my report that the NetRanger Director received and integrated alarms from a plurality of NSX sensors.

Q. (BY MR. MILLER) You're pointing to something when you state "here." What were you pointing to? 12:46:44

A. I'm pointing to, on page 12, we have under the column "NetRanger (public use or sale)," right there in that box, it says, "The NetRanger Director received and integrated alarms from a plurality of NSXs," so they're integrating them. 12:46:57

Q. What do you mean by "integrate" in that context?

A. In that context, the NetRanger Director, which would include the SMI daemon, HP OpenView, for example, that the alarms would come, you know, from the NSX sensor, through the SMI daemon, into HP OpenView, where it would then create an internal database record inside of HP OpenView that would then be used internally by open view to generate an icon on the screen. 12:47:14 12:47:36

If you had another event that was similar to the first one and that similarity may depend upon the different type of event, it may go into the same data structure, it may create a new 12:47:53

data structure for yet another icon, or it may just increment the count on the original icon.

Q. Which of those various actions do you believe constitutes integration, as claimed?

MS. BROWN: Objection, vague. 12:48:23

Q. (BY MR. MILLER) I'm sorry. I should have said "integrating, as claimed."

MS. BROWN: I'll also object that it's compound.

Q. (BY MR. MILLER) I'm going to repeat the question so it's clean for the record. 12:48:40

A. Okay.

Q. Which of the various actions that you defined a moment ago do you believe constitutes integrating as "integrating" is used in the claims of the patents-in-suit? 12:48:49

A. I would state that it would be the example of where the Director received two events that would be displayed and -- stored in the same data structure and displayed on the same icon on the screen. 12:49:08

Q. That icon that's displayed on the screen that can represent more than one event is called an alarm set icon? Turn to page 15, top of the page.

A. Yes. 12:49:48

Q. It says right there, "By default, if two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single," quote, "'alarm set,'" unquote, "icon." Do you see that? 12:50:08

A. Yes, I do.

Q. That's integration, in your opinion, as claimed by the patents-in-suit?

A. For -- yes, I use that definition for these claims with the integration. You're displaying them to the user, so that is my definition that I used. 12:50:16

Q. Your answer was not completely clear. This is -- this functionality, the one I just read, do you believe that that is integration, as it is claimed in the patents-in-suit? 12:50:38

MS. BROWN: Objection, asked and answered.

A. I would answer yes, because "integration" is a very broad term, and I believe that this would be included under the term of "integration" as I defined it for the claims in this suit. 12:50:55

Q. (BY MR. MILLER) Okay. As you defined it for the claims in this suit, what is the definition 12:51:14

data set that would then be provided as an icon. That was WheelGroup Soft Word that did that work. It ran within -- inside of HP OpenView.

HP OpenView has an extensible interface for third -- you know, for other applications to plug into. 14:59:29

Q. Okay. Do you understand what it means to combine references for an obviousness analysis?

MS. BROWN: Objection, calls for a legal conclusion. 14:59:39

A. I do not know what you mean by "combining references for obvious analysis."

Q. (BY MR. MILLER) Okay. Your attorney's objection makes a good point. Do you plan to provide any legal conclusions to the jury in this matter? 15:00:27

MS. BROWN: Objection, the document speaks for itself. His opinions are expressed in the document.

MR. MILLER: I'd like the witness to speak for himself. 15:00:41

Q. (BY MR. MILLER) Do you plan to provide any legal conclusions to the jury in this matter?

MS. BROWN: Objection, vague as to the phrase "legal conclusions." 15:00:48

A. Legal conclusions of what type?

Q. (BY MR. MILLER) Regarding the validity of the claims of the patents-in-suit.

A. I would state that the claims, as mentioned in my expert report, are not valid based upon the NetRanger system, and everything is documented in the expert report. 15:01:07

Q. And you don't know what an obviousness analysis is?

MS. BROWN: Objection, lacks foundation. The document speaks for itself. I'll just object further, the witness hasn't offered an obviousness opinion with regards to HP OpenView, so you're outside the bounds of the expert report, Counsel. 15:01:26 15:01:41

MR. MILLER: You're coaching. You know it.

A. As right here in the report -- and, again, I am not a lawyer -- it states in the report, "To establish obviousness under this test, one must show clear and convincing evidence that a person of ordinary skill in the art at the time of the invention, confronted by the same problem as the inventor and with no knowledge of the claimed invention, would select the recited elements from 15:01:52 15:02:06

the prior art and combine them in the claimed manner."

Q. (BY MR. MILLER) Okay. Are you doing that with NetRanger and HP OpenView? Are you performing an obviousness analysis as to any claim of the patents-in-suit by combining HP OpenView, which you say is a third-party product, and NetRanger? 15:02:15

MS. BROWN: Objection, the document speaks for itself. 15:02:28

A. I would point out in my expert report, right here, "It would have been obvious to one of ordinary skill to combine statistical profiling methods for anomaly detection," and it's described, "with NetRanger if a commercial grade was available." I don't see where I'm talking about HP OpenView when I'm stating this here. 15:02:56

Q. (BY MR. MILLER) Okay. So is the answer to my question yes or no?

MS. BROWN: Objection, asked and answered. 15:03:15

A. I believe I already stated that for HP OpenView...

I do not fully understand what you mean by "obviousness analysis of the claim in the 15:05:04

patents-in-suit by combining HP OpenView, which you say is a third-party product, and NetRanger."

Q. (BY MR. MILLER) You just don't understand the question?

A. I'm trying to understand what you're trying -- 15:05:20

Q. Do you know what "anticipation" is?

MS. BROWN: Objection, calls for a legal conclusion.

A. I do not know what "anticipation" from a legal term is. 15:05:31

Q. (BY MR. MILLER) How did you go about determining whether or not the claims of the patents-in-suit were invalid?

A. I discussed each of the claims with my legal counsel, going through, reading the claim, trying to understand what each term meant, which is -- they were very broad. They could mean any number of different things. 15:05:48

It was made aware to me at the time that those terms -- that there was a joint construction statement with a number of those terms in it. The definition of those terms was not, at this time -- at the time we were doing it, you know, fully specified as to which definition would be 15:06:07 15:06:21

used.

So going through and looking at the NetRanger system that I had, which looked awfully similar, upon first cursory review of the patent, it's like, this is my NetRanger system, with the exception that, you know, they're talking about statistical analysis, which NetRanger did not do. 15:06:44

Q. Did you -- were you told that there's a restriction or requirement that everything be taught by one reference, all aspects of the claim be taught by a single reference to do anticipation? 15:07:04

MS. BROWN: Objection, lacks foundation.

Q. (BY MR. MILLER) Were you told that?

A. I do not remember being told that. 15:07:17

Q. Did you apply that test for anticipation, that all of the elements claimed by each claim needed to be in one single reference?

MS. BROWN: Objection, vague as to "reference." Are you speaking to a document or to the product? 15:07:30

MR. MILLER: Renee, you're coaching the witness. We all know what we're talking about.

MS. BROWN: He does not know what you mean by "reference," and I'm telling you the 15:07:42

term is vague.

MR. MILLER: You just -- and there is a precise objection that you can state.

MS. BROWN: The term "reference" is vague -- 15:07:43

MR. MILLER: Thank you. You've stated your objection.

MS. BROWN: -- and I'm asking you to clarify it.

Q. (BY MR. MILLER) Sir, do you understand the question or not? 15:07:48

A. My understanding, when I looked at the claims, there was the supporting documentation, you know, in the patent. You know, the claims are the last piece on the end. Look at that, I didn't just look at the claims by themselves. 15:08:16

We had lengthy discussions over the claims, some of the information -- you know, the information that was in the patent. We may have discussed other references that were included and referenced by the patents. I don't remember which, what those references are. 15:08:34

Q. To determine whether any of the claims were invalid, did you compare the claims to the prior art? 15:08:55

MS. BROWN: Objection, vague.

A. I compared the claims primarily to the NetRanger system.

Q. (BY MR. MILLER) When you say you compared the claims to the NetRanger system, what, precisely, did you compare the claims to? I want to know exactly what you mean by "NetRanger system." 15:09:13

A. I compared the claims to all of my knowledge, to NetRanger, being the original author, architect, original coder of the NetRanger system, being a founder of WheelGroup, going through the user's manuals, refreshing my memory, going through all the documentation that we've discussed here today; and going through that, to me, it was apparent there were the -- when I reached those conclusions, that's why I said NetRanger was already doing what I stated NetRanger was already doing. 15:09:43 15:10:04

Q. Based on your knowledge of the product as a coder of the product, correct?

A. Correct, based upon my knowledge as the inventor of the system, of the NetRanger system -- 15:10:22

Q. Based on all of the documents taken together?

A. Based on all of the documents taken together. 15:10:37

Q. Okay.

A. You know, that also includes my memories of customers using the system.

Q. I see. So undocumented memories of customer applications of NetRanger, that was included as well? 15:10:58

MS. BROWN: Objection, calls for speculation.

Q. (BY MR. MILLER) You included undocumented recollections of NetRanger deployments by NetRanger customers in your invalidity analysis? 15:11:05

MS. BROWN: Objection, calls for speculation. The document speaks for itself, if you'd care to point him to anything that you are alleging is in the expert report. 15:11:23

A. For the undocumented memories that we were discussing goes back to those SQL queries, which we have already discussed.

Q. (BY MR. MILLER) Okay. If you could turn to Exhibit D of your report, and if you could turn to page 74986 of Exhibit 464 as well. My question, sir, is this: Is there a difference between Figure 1.6 in Exhibit 464 and the first page of your Exhibit D? 15:11:41

MS. BROWN: Objection, the document 15:12:35

speaks for itself.

A. Are you asking me if this is the exact same image both in the user's manual and on this architecture?

Q. (BY MR. MILLER) Yeah. Is there a difference between the two? 15:12:49

A. You know, the pictures look the same.

Q. Okay. Where is the next page of Exhibit D to your report found in the 1.3.1 manual?

MS. BROWN: Objection, lacks foundation. 15:13:13

Q. (BY MR. MILLER) You wouldn't dispute my representation that it is not in the manual, would you?

A. No, if you do not find it in the manual. 15:13:27

Q. You state that one Director could report up to a higher Director, higher-tier Director, at page 38 of your report?

A. Yes, that is true.

Q. Is what's described here at the top of 74986, which refers to Figure 1.6 -- is it incorrect? It says, "In addition to providing performance benefits and fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines 15:13:49 15:14:09

Q. (BY MR. MILLER) Then you go on --

MS. BROWN: Mr. Teal was in the middle of a sentence, and he's entitled to finish his sentence, if he wishes to.

Q. (BY MR. MILLER) Then you go on to say that commercial-grade anomaly detection software did not exist in 1997, right? 15:49:50

A. I had not seen, or was aware of, any commercial-grade software, based upon the definition that is -- I had not seen any commercial customers of ours using it. To my knowledge, none of our sales forces encountered any product using statistical anomaly detection. 15:50:09

The only products in 1997 that we encountered, to my recollection, is the ISS RealSecure product. 15:50:22

Q. I'm not trying to trick you, sir. You say it would be obvious to combine NetRanger with statistical anomaly detection if commercial statistical anomaly detection existed, right? 15:50:38

A. That's what I'm stating.

Q. And you say commercial-grade statistical anomaly detection software didn't exist in 1997, right?

A. Yes, that's what I state. 15:50:49

Q. So if commercial-grade statistical anomaly detection software did not exist in 1997, then the combination of statistical anomaly detection software and NetRanger would not have been obvious in 1997. Is that a fair conclusion to draw? 15:51:04

MS. BROWN: Objection, lacks foundation.

A. I specifically said commercial-grade software.

Q. (BY MR. MILLER) Yeah. 15:51:17

A. It's a different answer if you are building a research system, mainly because, based upon my experience, people building research systems, the more engines, analysis engines and so forth you had, the better Ph.D. thesis it would 15:51:32 appear, the better papers you could present.

I was interested in building a commercial-grade product and not a research-type product.

Q. That does not answer my question, so let 15:51:51 me try again. You said it would be obvious to combine NetRanger and statistical anomaly detection, but only if a commercial-grade version of statistical anomaly detection software existed, right? 15:52:08

MS. BROWN: Objection --

Q. (BY MR. MILLER) That's what you say in paragraph 60.

A. Yes, that is what I state. I state right here that we would combine it if commercial-grade software implementing such anomaly detection had existed in 1997. 15:52:15

Q. Okay. Then you go down to paragraph 61 and you say commercial-grade statistical anomaly detection software didn't exist, right, in 1997? 15:52:29

A. Yes, I state right here in my report that I do not believe that commercial-grade system for statistical anomaly detection existed in 1997 that was suitable for inclusion in NetRanger.

Q. So isn't the condition that you establish in paragraph 60 not satisfied; in essence, the combination of NetRanger and statistical anomaly detection would not be obvious? 15:52:50

MS. BROWN: Objection, lacks foundation. 15:53:06

A. In there, I was referring to the existence that NetRanger is a commercial-grade system. I did not -- in fact, I tried to use another engine in the early development phases of NetRanger. It didn't work well. It didn't meet 15:53:35

what I needed for a commercial-grade product, so, therefore, I did not use it. I was -- if there had been a commercial-grade statistical anomaly detection system, I may have included it in NetRanger in 1997. 15:54:02

Q. (BY MR. MILLER) Okay. But, sir, you're not answering my question. You set up a condition for obviousness in paragraph 60. Isn't that true?

MS. BROWN: Objection, lacks foundation. 15:54:16

Q. (BY MR. MILLER) You see what you say there?

A. Basically, I'm stating that if you're building a commercial-grade system -- I mean --

Q. You say, it would have been obvious to one of ordinary skill at the time to combine a statistical profiling method for anomaly detection such as those described in statistical methods in EMERALD 1997 with the NetRanger system, if, "if" commercial-grade software implementing such an anomaly detection system had existed in 1997. That's what you say in your report. Is that true or not? 15:54:37 15:55:00

A. That is correct. That is what I state in my report. 15:55:11

Q. You go on to say that that commercial-grade software did not exist. You say that in paragraph 61, right?

A. That is correct.

Q. So, then, there's no way on earth that it would be obvious to combine the two, based on what you say in paragraph 60. 15:55:19

MS. BROWN: Objection, lacks foundation, misstates the expert report, paragraph 61 in particular. 15:55:34

Q. (BY MR. MILLER) Go ahead and explain it to me, sir.

A. In 61, I state, the first sentence, which is, "However, the needs of a commercial system such as NetRanger were very different than a research system. In particular, when performing real-time network intrusion detection" -- 15:55:45

Q. You've got to go slower for her.

A. Okay.

-- "it was of paramount importance that the software analyzing the network traffic run quickly in order to be able to keep up with the incoming stream of network packets." 15:56:03

Q. You can go faster.

A. "WheelGroup actually investigated adding 15:56:22

wanted it to.

THE VIDEOGRAPHER: We've got five minutes left on the tape.

Q. (BY MR. MILLER) Did you ever try to improve upon Mr. Smaha's software? 16:05:46

A. Do you define as improving his software in particular, or writing my own signatures to do what his did?

Q. I thought that you had characterized his software as anomaly detection. Did you ever try to write your own commercially viable and sound statistical anomaly detection engine? 16:06:07

A. I did not. As I previously stated, I found that I could detect all the signatures that I needed with signature analysis. 16:06:26

Q. Isn't the shortcoming of signature-based analysis that a person intent on misuse can simply design an attack that there is no signature for?

MS. BROWN: Objection, calls for speculation, incomplete hypothetical. 16:06:44

A. That is correct. If you have an attack where there is no signature in the engine, just like antivirus engines, that is one of the shortcomings of a signature misuse engine.

Q. (BY MR. MILLER) And that's one of the 16:07:02

alleged strengths of a statistical anomaly detection engine, is that it can detect attacks that have never been seen before.

A. I would state that it might be able to detect attacks that have never been seen before. 16:07:15
The fundamental problem that I had seen in using statistical detection methods is, of course, training, you establish profiles. If the attacker is already in the network, he becomes part of the profile. Trying to get your operators at your 16:07:37
commercial companies to be able to configure and train the system properly for their environment had a lot of shortcomings. It was hard to do.

Q. If it could be done, would it have -- if an appropriate statistical anomaly detection engine 16:08:01
could have been created, would it have improved NetRanger?

MS. BROWN: Objection, calls for speculation, incomplete hypothetical.

A. If you could have built a commercially 16:08:19
reliable straight anomaly detection engine, it would have improved NetRanger. As I stated before, I do not believe -- I was not aware of any such thing that existed that could be included to NetRanger in 1997. 16:08:42

Q. (BY MR. MILLER) And you didn't attempt to design and build your own statistical anomaly detection engine that would meet all the requirements that you've laid out that would be commercially viable -- commercial-grade, I'm sorry -- even though it would improve NetRanger? 16:08:54

A. I did not take the time. Again, as I just previously stated, it is very hard to design a commercial-grade statistical anomaly detection engine that could be used, you know, by companies on a regular basis. 16:09:16

THE VIDEOGRAPHER: I need to change tapes. We're off the record at 4:09 p.m. This is the end of Tape No. 6.

(Recess taken at 4:09 p.m.) 16:09:33

THE VIDEOGRAPHER: Stand by, please. We're back on the record at 4:11 p.m. This is the beginning of Tape No. 7.

Q. (BY MR. MILLER) Mr. Teal, what test did you apply in determining or in reaching your conclusion that it would be obvious to combine the teachings of Statistical Methods and EMERALD '97 with NetRanger to render obvious the claims of the '212 patent? 16:11:24

A. I would refer you to my report, 16:11:56

paragraph 56, where I state, "I understand that one must show by clear and convincing evidence that a person of ordinary skill in the art at the time of invention, confronted by the same problem as the inventor and with no knowledge of the claimed invention, would select the recited elements from the prior art and combine them in the claimed manner."

Q. What is your suggestion for a motivation to combine those references? 16:12:44

A. You know, I state, "In other words, one must avoid the use of hindsight and instead identify in the art prior to the invention some suggestion or motivation, before the invention itself was made, to make the new combination," and I'll refer you to 16:13:24 paragraph 61 where, while designing NetRanger I attempted to put in another engine, and it didn't work. And, at that time, I was not aware of these patents.

I was aware of prior art regarding 16:13:47 different statistical anomaly detection engines, signature analysis engines, and that is why, when I was designing NetRanger, where I attempted to combine the two engines in one product.

Q. Where is the suggestion or motivation to 16:14:09

combine NetRanger with EMERALD or statistical analysis, the NIDES paper, in any document relating to NetRanger?

MS. BROWN: Objection, calls for a legal conclusion. 16:14:26

A. On there, I chose NetStalker from Haystack Labs for my initial attempt to combine them. It was an engine. We knew Steve Smaha. As I previously stated, I did not know the individuals at SRI very well. Maybe if I had known them, I might have contacted them. I do not know. 16:14:50

Q. (BY MR. MILLER) My question was: Where is the suggestion or motivation to combine NetRanger with the EMERALD 1997 paper or the NIDES paper provided in any of the NetRanger documentation? 16:15:09

A. I am implying that since I attempted to include one engine, it could just as well have been the EMERALD or the NIDES engine that I had tried to produce.

Q. But I'm asking you where in any of the NetRanger papers it provides any suggestion or motivation to combine NetRanger with the SRI statistical engine. 16:15:28

MS. BROWN: Objection, if you'd like to point him to some place in his expert report 16:15:42

where you're claiming he stated this, it's outside the scope of his expert report. It's not in here.

Q. (BY MR. MILLER) I'll point you to the paragraph that you read to me, paragraph 56. "In other words, one must avoid the use of hindsight and instead identify in the art prior to the invention some suggestion or motivation, before the invention itself was made, to make the new combination." 16:15:59

MS. BROWN: That statement --

Q. (BY MR. MILLER) So please provide me with the suggestion or motivation found in NetRanger to combine it with the SRI work. 16:16:15

MS. BROWN: Counsel, as you've just pointed out, paragraph 56 doesn't refer to NetRanger. It refers to the prior art. 16:16:28

MR. MILLER: Your objection is noted. Okay. Your objection is noted.

A. You know, in there, I am not stating with regards to NetRanger in paragraph 56. I state in paragraph 61 that I attempted to integrate the statistical analysis engine in NetRanger -- 16:16:50

Q. (BY MR. MILLER) So --

A. -- and did not do so.

Q. I'm sorry.

Other than your purported attempt to 16:17:02